'780 Patent

US005708780A

United States Patent [19]
Levergood et al.

[11] **Patent Number: 5,708,780**
[45] **Date of Patent: Jan. 13, 1998**

[54] **INTERNET SERVER ACCESS CONTROL AND MONITORING SYSTEMS**

[75] Inventors: **Thomas Mark Levergood**, Hopkinton; **Lawrence C. Stewart**, Burlington; **Stephen Jeffrey Morris**, Westford; **Andrew C. Payne**, Lincoln; **George Winfield Treese**, Newton, all of Mass.

[73] Assignee: **Open Market, Inc.**, Cambridge, Mass.

[21] Appl. No.: **474,096**

[22] Filed: **Jun. 7, 1995**

[51] **Int. Cl.**[6] **G06F 15/56**

[52] **U.S. Cl.** **395/200.12**; 395/200.15

[58] **Field of Search** 395/200.11, 200.12, 395/200.02, 200.05, 200.06, 200.09, 200.15; 380/23, 24, 25, 49; 340/825.34

[56] **References Cited**

U.S. PATENT DOCUMENTS

5,347,632	9/1994	Filepp et al.	395/200
5,544,322	8/1996	Cheng et al.	395/200.12
5,560,008	9/1996	Johnson et al.	395/200.09
5,577,209	11/1996	Boyle et al.	395/200.06

FOREIGN PATENT DOCUMENTS

0 456 920	11/1991	European Pat. Off. .	
0 645 688	3/1995	European Pat. Off. .	
WO 94/03859	2/1994	WIPO	G06F 13/14
WO 94/03959	2/1994	WIPO .	

OTHER PUBLICATIONS

Bina et al., Secure Access to Data over the Internet, 1994, pp. 99–102, IEEE.

Kiuchi et al., C-HTTP—the Development of a Secure, Closed HTTP based Network on the Internet, 1996, pp. 64–75, IEEE.

Ramanathan, Srinivas, et al., "Architectures for Personalized Multimedia," IEEE Multimedia, vol. 1, No. 1, Computer Society, pp. 37–46, 1994.

Choudhury, Abhijit K., et al., "Copyright Protection for Electronic Publishing Over Computer Networks," IEEE Network, The Magazine of Computer Communications, vol. 9, No. 3, pp. 12–20, May 1995.

Netscape Products, "Open and Secure Internet Software" Internet Sep. 18, 1995, pp. 1–2.

Merchant System: Overview, "Netscape Merchant System Data Sheet" Internet, Sep. 18, 1995, pp. 1–3.

Internet Applications Customer Showcase, "Customer Showcase" Internet, Sep. 18, 1995., pp. 1–2.

The Server–Application Function and Netscape Server API, "The Netscape Server API" Netscape Products Internet, Sep. 18, 1995, pp. 1–11.

The Object–Oriented Paradigm of Server Configuration, "The Object–Oriented Paradigm of Server Configuration" Internet, Sep. 18, 1995, p. 102.

Verisign Redirection Information, "Important Announcement" Internet, Sep. 18, 1995, p. 1.

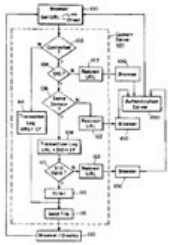
(List continued on next page.)

Primary Examiner—William M. Treat
Assistant Examiner—Patrice L. Winder
Attorney, Agent, or Firm—Hamilton, Brook, Smith & Reynolds, P.C.

[57] **ABSTRACT**

This invention relates to methods for controlling and monitoring access to network servers. In particular, the process described in the invention includes client-server sessions over the Internet involving hypertext files. In the hypertext environment, a client views a document transmitted by a content server with a standard program known as the browser. Each hypertext document or page contains links to other hypertext pages which the user may select to traverse. When the user selects a link that is directed to an access-controlled file, the server subjects the request to a secondary server which determines whether the client has an authorization or valid account. Upon such verification, the user is provided with a session identification which allows the user to access to the requested file as well as any other files within the present protection domain.

45 Claims, 7 Drawing Sheets



'780 Patent Disputed Claim Terms

Eighteen disputed terms, in groups relating to:

1. Path Name In A URL
2. Session
3. Hypertext
4. Authentication Server
5. Means-Plus-Function Elements

1. Path Name In A URL Terms

- "path name in a uniform resource locator"
- "appending…[the session identifier]…as part of a…path name in a uniform resource locator"

1. Path Name In A URL Terms

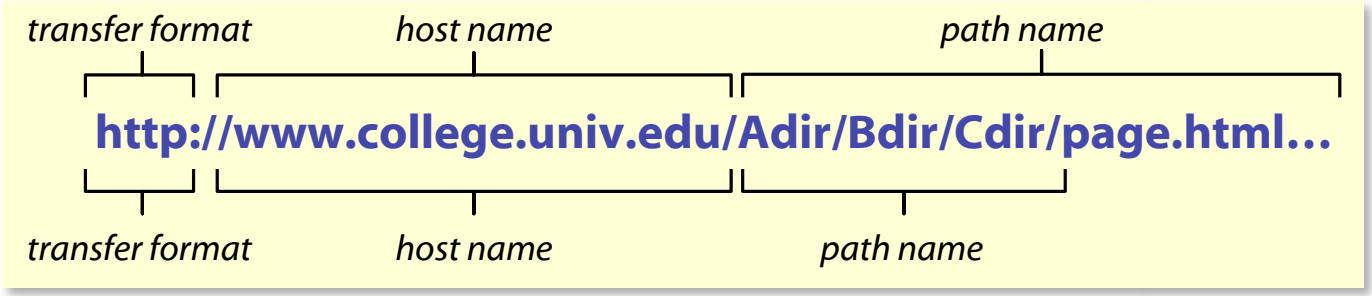
"path name in a uniform resource locator"

Soverain's Construction	Defendants' Construction
a sequence of zero or more elements that follows the host address in a URL	the name of the directories leading to the file identified by the URL nothing after the file name is part of the path name

1. Path Name In A URL Terms

"path name in a uniform resource locator"

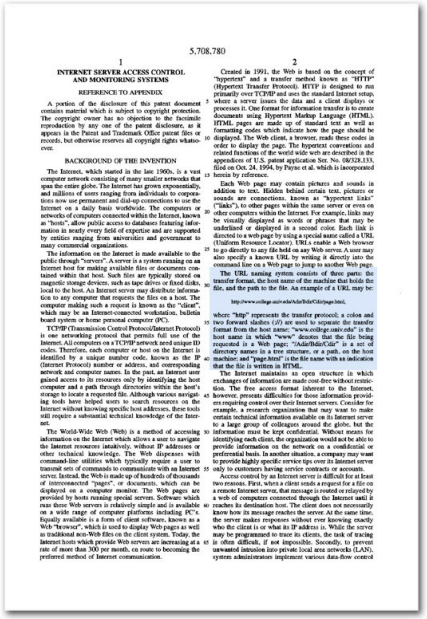
Soverain's construction: path name = URL part following the host name



Defendants' construction: path name = directory tree before the file name

Soverain's construction is consistent with the ordinary meaning of the term in the art, and with the intrinsic record.

1. Path Name In A URL Terms



5,708,780

1

INTERNET SERVER ACCESS CONTROL AND MONITORING SYSTEMS

REFERENCE TO APPENDIX

A portion of the disclosure of this patent document contains material which is subject to copyright protection. The copyright owner has no objection to the facsimile reproduction by any one of the patent disclosure, as it appears in the Patent and Trademark Office patent files or records, but otherwise reserves all copyright rights whatsoever.

BACKGROUND OF THE INVENTION

The Internet, which started in the late 1960s, is a vast computer network consisting of many smaller networks that span the entire globe. The Internet has grown exponentially, and millions of users ranging from individuals to corporations now use permanent and dial-up connections to use the Internet on a daily basis worldwide. The computers or networks of computers connected within the Internet, known as "hosts", allow public access to databases featuring information in nearly every field of expertise and are supported by entities ranging from universities and government to many commercial organizations.

The information on the Internet is made available to the public through "servers". A server is a system running on an Internet host for making available files or documents contained within that host. Such files are typically stored on magnetic storage devices, such as tape drives or fixed disks, local to the host. An Internet server may distribute information to any computer that requests the files on a host. The computer making such a request is known as the "client", which may be an Internet-connected workstation, bulletin board system or home personal computer (PC).

TCP/IP (Transmission Control Protocol/Internet Protocol) is one networking protocol that permits full use of the Internet. All computers on a TCP/IP network need unique ID codes. Therefore, each computer or host on the Internet is identified by a unique number code, known as the IP (Internet Protocol) number or address, and corresponding network and computer names. In the past, an Internet user gained access to its resources only by identifying the host computer and a path through directories within the host's storage to locate a requested file. Although various navigating tools have helped users to search resources on the Internet without knowing specific host addresses, these tools still require a substantial technical knowledge of the Internet.

The World-Wide Web (Web) is a method of accessing information on the Internet which allows a user to navigate the Internet resources intuitively, without IP addresses or other technical knowledge. The Web dispenses with command-line utilities which typically require a user to transmit sets of commands to communicate with an Internet server. Instead, the Web is made up of hundreds of thousands of interconnected "pages", or documents, which can be displayed on a computer monitor. The Web pages are provided by hosts running special servers. Software which runs these Web servers is relatively simple and is available on a wide range of computer platforms including PC's. Equally available is a form of client software, known as a Web "browser", which is used to display Web pages as well as traditional non-Web files on the client system. Today, the Internet hosts which provide Web servers are increasing at a rate of more than 300 per month, on route to becoming the preferred method of Internet communication.

2

Created in 1991, the Web is based on the concept of "hypertext" and a transfer method known as "HTTP" (Hypertext Transfer Protocol). HTTP is designed to run primarily over TCP/IP and uses the standard Internet setup, where a server issues the data and a client displays or processes it. One format for information transfer is to create documents using Hypertext Markup Language (HTML). HTML pages are made up of standard text as well as formatting codes which indicate how the page should be displayed. The Web client, a browser, reads these codes in order to display the page. The hypertext conventions and related functions of the world wide web are described in the appendices of U.S. patent application Ser. No. 08/328,133, filed on Oct. 24, 1994, by Payne et al. which is incorporated herein by reference.

Each Web page may contain pictures and sounds in addition to text. Hidden behind certain text, pictures or sounds are connections, known as "hypertext links" ("links"), to other pages within the same server or even on other computers within the Internet. For example, links may be visually displayed as words or phrases that may be underlined or displayed in a second color. Each link is directed to a web page by using a special name called a URL (Uniform Resource Locator). URLs enable a Web browser to go directly to any file held on any Web server. A user may also specify a known URL by writing it directly into the command line on a Web page to jump to another Web page.

The URL naming system consists of three parts: the transfer format, the host name of the machine that holds the file, and the path to the file. An example of a URL may be:

http://www.college.univ.edu/Adir/Bdir/Cdir/page.html,

where "http" represents the transfer protocol; a colon and two forward slashes (://) are used to separate the transfer format from the host name; "www.college.univ.edu" is the host name in which "www" denotes that the file being requested is a Web page; "/Adir/Bdir/Cdir" is a set of directory names in a tree structure, or a path, on the host machine; and "page.html" is the file name with an indication that the file is written in HTML.

The Internet maintains an open structure in which exchanges of information are made cost-free without restriction. The free access format inherent to the Internet, however, presents difficulties for those information providers requiring control over their Internet servers. Consider for example, a research organization that may want to make certain technical information available on its Internet server to a large group of colleagues around the globe, but the information must be kept confidential. Without means for identifying each client, the organization would not be able to provide information on the network on a confidential or preferential basis. In another situation, a company may want to provide highly specific service tips over its Internet server only to customers having service contracts or accounts.

Access control by an Internet server is difficult for at least two reasons. First, when a client sends a request for a file on a remote Internet server, that message is routed or relayed by a web of computers connected through the Internet until it reaches its destination host. The client does not necessarily know how its message reaches the server. At the same time, the server makes responses without ever knowing exactly who the client is or what its IP address is. While the server may be programmed to trace its clients, the task of tracing is often difficult, if not impossible. Secondly, to prevent unwanted intrusion into private local area networks (LAN), system administrators implement various data-flow control

('780 Patent, 2:28-41)

The URL naming system consists of three parts: the transfer format, the host name of the machine that holds the file, and the path to the file. An example of a URL may be:

http://www.college.univ.edu/Adir/Bdir/Cdir/page.html,

where "http" represents the transfer protocol; a colon and two forward slashes (://) are used to separate the transfer format from the host name; "www.college.univ.edu" is the host name in which "www" denotes that the file being requested is a Web page; "/Adir/Bdir/Cdir" is a set of directory names in a tree structure, or a path, on the host machine; and "page.html" is the file name with an indication that the file is written in HTML.

Defendants' construction fails because:

1. their argument that the ordinary meaning of the term "is overridden by express definition in the patent" contradicts the above disclosure, on which they rely

2. the patent does not define the file name as a fourth URL part, excluded from the path name

1. Path Name In A URL Terms

"appending … as part of a path name in a URL"

Soverain's Construction	Defendants' Construction
tagging, adding, affixing or supplementing [the session identifier] to the URL as part of a path name	tagging, adding, affixing or supplementing within or after the path name (but before the file name)

Defendants' Position: Session identifier can be placed anywhere in the pathname:

http://www.college.univ.edu/SID/Adir/Bdir/Cdir/page.html
http://www.college.univ.edu/Adir/Bdir/Cdir/SID/page.html
http://www.college.univ.edu/Adir/SID/Bdir/Cdir/page.html

Except at the end, (where it is used in Amazon's web site)

http://www.college.univ.edu/Adir/Bdir/Cdir/page.html/SID

2. Session-Related Terms

- "session"
- "session identifier"
- "authorization identifier"

2. Session-Related Terms

"session"

Soverain's Construction	Defendants' Construction
a series of requests and responses to perform a complete task or set of tasks between a client and a server system	an uninterrupted series of requests and responses between (1) a specific client (identified by its network address and user) and (2) a specific server system

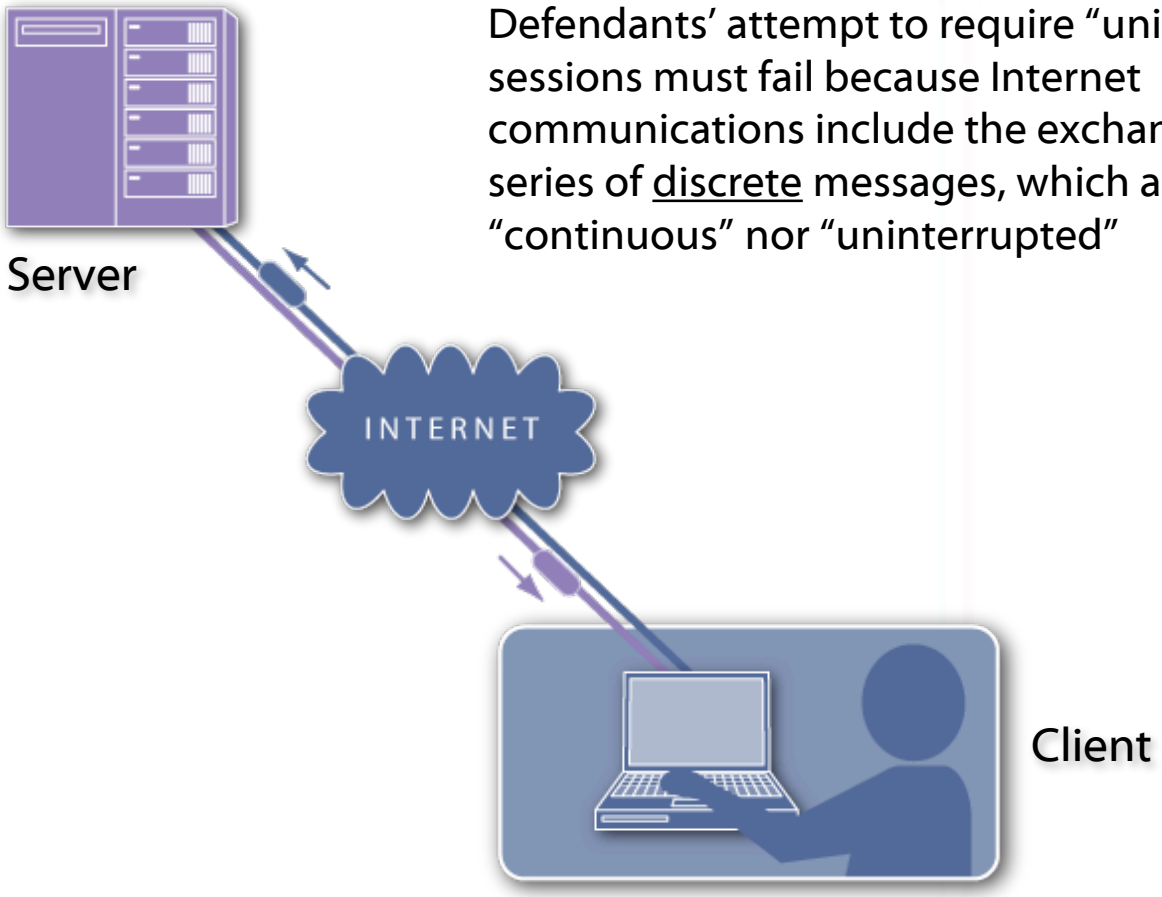
2. Session-Related Terms

Examples of Internet Session

- A complete task in a session is illustrated by the Internet Purchase Example in Soverain's Tutorial presentation, where a client purchases several items in a shopping basket.
- Discrete tasks in a session may involve viewing one or more articles in a server system.

2. Session-Related Terms

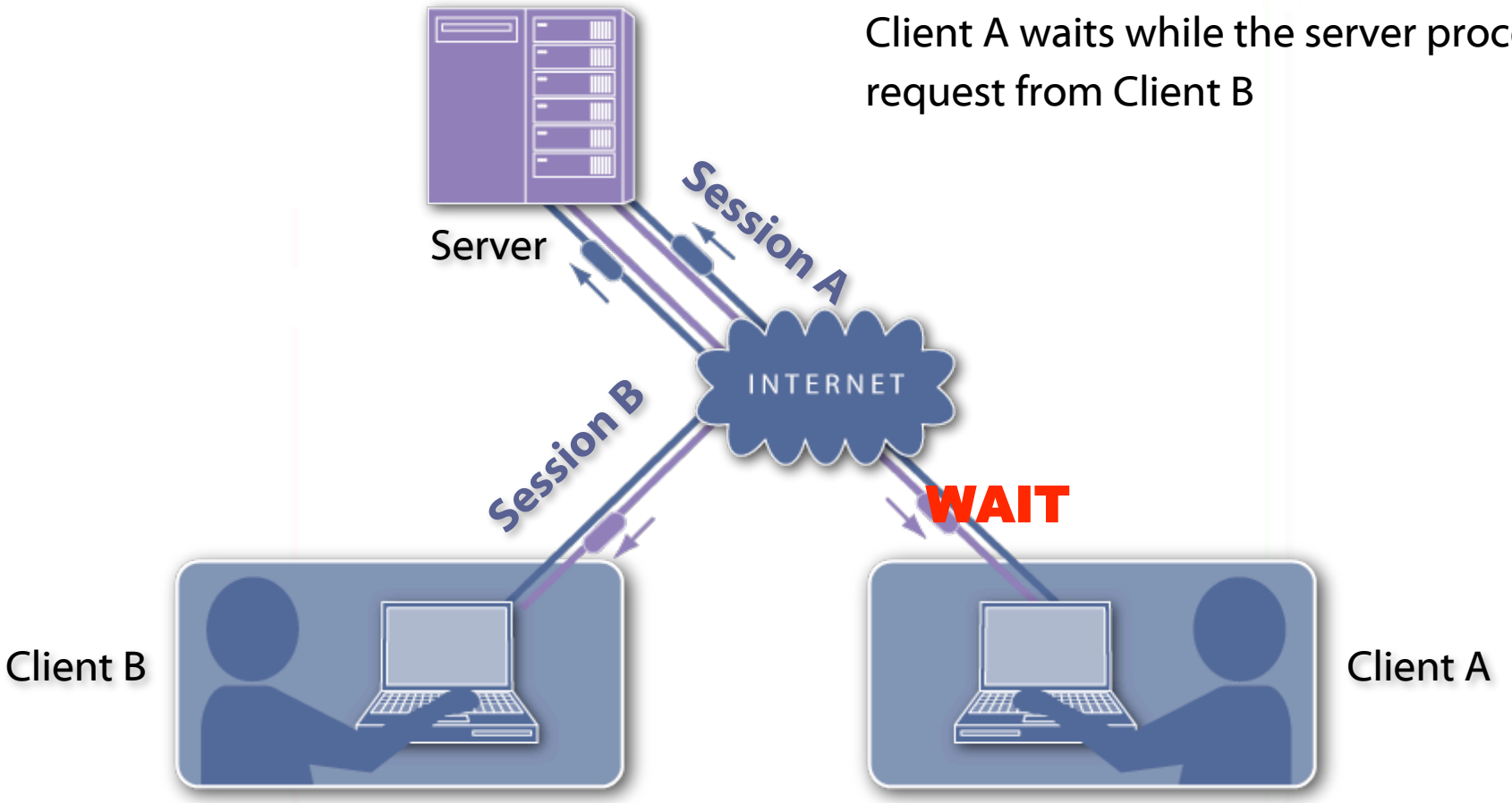
Internet Sessions Use Discrete Communications



Defendants' attempt to require "uninterrupted" sessions must fail because Internet communications include the exchange of a series of discrete messages, which are neither "continuous" nor "uninterrupted"

2. Session-Related Terms

Sessions With Multiple Clients May Be "interrupted"



2. Session-Related Terms

The Defendants' Attempt to Define a "Session" in Terms of User Identification Fails:

Legally, because:

- Defendants are improperly attempting to read into the claims a feature of a preferred embodiment
- User identification is <u>not</u> part of the definition of a "session" under claim differentiation principles

Factually, because:

- Defendants erroneously rely on a discussion of <u>one</u> aspect of the invention
- The specification discloses sessions with different authentication level requirements (col. 6:36-47); user identification is one option, which cannot be part of the definition of a "session"

2. Session-Related Terms

Defendants' Attempt to Import Identification by User of a "Session" Into the Claims Fails Legally

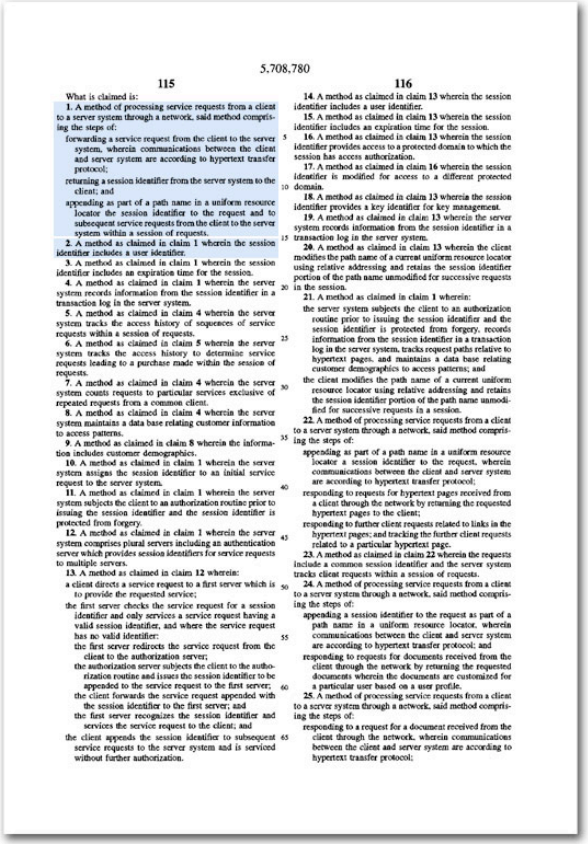
Even if a patent describes only a single embodiment (which is not the case here), a long line of Federal Circuit decisions has:

> *"…expressly rejected the contention that . . . the claims of the patent must be construed as being limited to that embodiment."*

Liebel-Flarsheim Co. v. Medrad, Inc., 358 F.3d 898, 906 (Fed. Cir. 2004)
(Citing *ACTV, Inc. v. Walt Disney Co.*, 346 F.3d 1082, 1091 (Fed. Cir. 2003); *Apex Inc. v. Raritan Computer, Inc.*, 325 F.3d 1364, 1377 (Fed. Cir. 2003); *Altiris, Inc. v. Symantec Corp., 318 F.3d 1363, 1373 (Fed. Cir. 2003); Tex. Digital Sys., Inc. v. Telegenix, Inc.*, 308 F.3d 1193, 1204-05 (Fed. Cir. 2002); *Teleflex, Inc. v. Ficosa N. Am. Corp.*, 299 F.3d 1313, 1327 (Fed. Cir. 2002); *SRI Int'l v. Matsushita Elec. Corp. of Am.*, 775 F.2d 1107, 1121 n. 14 (Fed. Cir. 1985) (en banc)).

2. Session-Related Terms

Adding User Identification As the Only New Element in a Dependent Claim Gives Rise to a Presumption That It Is Not Part of the Definition of a "Session"



5,708,780

115

What is claimed is:

1. A method of processing service requests from a client to a server system through a network, said method comprising the steps of:

forwarding a service request from the client to the server system, wherein communications between the client and server system are according to hypertext transfer protocol;

returning a session identifier from the server system to the client; and

appending as part of a path name in a uniform resource locator the session identifier to the request and to subsequent service requests from the client to the server system within a session of requests.

2. A method as claimed in claim 1 wherein the session identifier includes a user identifier.

3. A method as claimed in claim 1 wherein the session identifier includes an expiration time for the session.

4. A method as claimed in claim 1 wherein the server system records information from the session identifier in a transaction log in the server system.

5. A method as claimed in claim 4 wherein the server system tracks the access history of sequences of service requests within a session of requests.

6. A method as claimed in claim 5 wherein the server system tracks the access history to determine service requests leading to a purchase made within the session of requests.

7. A method as claimed in claim 4 wherein the server system counts requests to particular services exclusive of repeated requests from a common client.

8. A method as claimed in claim 4 wherein the server system maintains a data base relating customer information to access patterns.

9. A method as claimed in claim 8 wherein the information includes customer demographics.

10. A method as claimed in claim 1 wherein the server system assigns the session identifier to an initial service request to the server system.

11. A method as claimed in claim 1 wherein the server system subjects the client to an authorization routine prior to issuing the session identifier and the session identifier is protected from forgery.

12. A method as claimed in claim 1 wherein the server system comprises plural servers including an authentication server which provides session identifiers for service requests to multiple servers.

13. A method as claimed in claim 12 wherein:

a client directs a service request to a first server which is to provide the requested service;

the first server checks the service request for a session identifier and only services a service request having a valid session identifier, and where the service request has no valid identifier:

the first server redirects the service request from the client to the authorization server;

the authorization server subjects the client to the authorization routine and issues the session identifier to be appended to the service request to the first server;

the client forwards the service request appended with the session identifier to the first server; and

the first server recognizes the session identifier and services the service request to the client; and

the client appends the session identifier to subsequent service requests to the server system and is serviced without further authorization.

116

14. A method as claimed in claim 13 wherein the session identifier includes a user identifier.

15. A method as claimed in claim 13 wherein the session identifier includes an expiration time for the session.

16. A method as claimed in claim 13 wherein the session identifier provides access to a protected domain to which the session has access authorization.

17. A method as claimed in claim 16 wherein the session identifier is modified for access to a different protected domain.

18. A method as claimed in claim 13 wherein the session identifier provides a key identifier for key management.

19. A method as claimed in claim 13 wherein the server system records information from the session identifier in a transaction log in the server system.

20. A method as claimed in claim 13 wherein the client modifies the path name of a current uniform resource locator using relative addressing and retains the session identifier portion of the path name unmodified for successive requests in the session.

21. A method as claimed in claim 1 wherein:

the server system subjects the client to an authorization routine prior to issuing the session identifier and the session identifier is protected from forgery, records information from the session identifier in a transaction log in the server system, tracks request paths relative to hypertext pages, and maintains a data base relating customer demographics to access patterns; and

the client modifies the path name of a current uniform resource locator using relative addressing and retains the session identifier portion of the path name unmodified for successive requests in a session.

22. A method of processing service requests from a client to a server system through a network, said method comprising the steps of:

appending as part of a path name in a uniform resource locator a session identifier to the request, wherein communications between the client and server system are according to hypertext transfer protocol;

responding to requests for hypertext pages received from a client through the network by returning the requested hypertext pages to the client;

responding to further client requests related to links in the hypertext pages; and tracking the further client requests related to a particular hypertext page.

23. A method as claimed in claim 22 wherein the requests include a common session identifier and the server system tracks client requests within a session of requests.

24. A method of processing service requests from a client to a server system through a network, said method comprising the steps of:

appending a session identifier to the request as part of a path name in a uniform resource locator, wherein communications between the client and server system are according to hypertext transfer protocol; and

responding to requests for documents received from the client through the network by returning the requested documents wherein the documents are customized for a particular user based on a user profile.

25. A method of processing service requests from a client to a server system through a network, said method comprising the steps of:

responding to a request for a document received from the client through the network, wherein communications between the client and server system are according to hypertext transfer protocol;

('780 Patent, claims 1 and 2)

1. A method of processing service requests from a client to a server system through a network, said method comprising the steps of:

forwarding a service request from the client to the server system, wherein communications between the client and server system are according to hypertext transfer protocol;

returning a session identifier from the server system to the client; and

appending as part of a path name in a uniform resource locator the session identifier to the request and to subsequent service requests from the client to the server system within a session of requests.

2. A method as claimed in claim 1 wherein the session identifier includes a user identifier.

2. Session-Related Terms

"session identifier"

Soverain's Construction	Defendants' Construction
a text string that identifies a session	a value [1]with multiple fields [2]whose cryptographic authentication [3]indicates to an access-controlling server that [4]the client identified in the session identifier is [5]authorized to access [6]the requested file